PROJECTIVE RESOLUTION OF MODULES OVER THE NONCOMMUTATIVE ALGEBRA

Tomohiro Fukaya*

Abstract

We give an explicit algorithm to compute a projective resolution of a module over the noncommutative ring based on the noncommutative Gröbner bases theory.

Introduction

Let K be a field and Γ be a ring over K. We generally assume that Γ has a unit, $\epsilon\colon K \to \Gamma$, as well as an augmentation $\eta\colon \Gamma \to K$. For graded Γ-module M and N, $\mathrm{Ext}_{\Gamma}^{*,*}(M,N)$ is defined with a projective resolution of M. This Ext-functor appears in various areas. In algebraic topology, it appears as a E_2-terms of the Adams spectral sequence, which is one of the most important tools to compute homotopy sets. Especially, it is given by $\mathrm{Ext}_{\mathcal{A}_p}^{*,*}(\mathbb{F}_p,\mathbb{F}_p)$that E_2-terms of the spectral sequence which converges to the stable homotopy groups of the sphere ${}_{(p)}\Pi_S^*$. Here $\mathcal{A}_p$ denotes the mod p Steenrod algebra and

$$\begin{aligned} \Pi_S^* &= \bigoplus_k \lim_{n\to\infty} [S^{n+k}, S^n] \\ {}_{(p)}\Pi_S^* &= \Pi_S^*/\{\text{elements of finite order prime to } p\}. \end{aligned}$$

The study of the stable homotopy groups of sphere has a long history, so many tools has been developed. For example, there exists a spectral sequence converging to $\mathrm{Ext}_{\mathcal{A}_p}^{*,*}(\mathbb{F}_p,\mathbb{F}_p)$.

In this paper, we study an elementary algorithm to compute the Ext-functor directly from its definition, that is, to compute a projective resolution of Γ-modules.

2000 *Mathematics Subject Classification.* Primary 18G15; Secondary 55S10.

Key words and phrases. Steenrod algebra, Projective resolution, Gröbner basis.

*The author is supported by Grant-in-Aid for JSPS Fellows (19·3177) from Japan Society for the Promotion of Science.

A brief explanation of Ext-functor can be seen in the section 9.2 of [3]. We fix a positive integer k. It is enough to compute $\mathrm{Ext}^{s,t}(M,-)$ for $0 \leq t \leq k$ that we have a sequence of degree-preserving Γ-homomorphisms between graded Γ modules

$$0 \leftarrow M \xleftarrow{\epsilon} P_0 \xleftarrow{d_0} P_1 \xleftarrow{d_1} P_2 \xleftarrow{d_2} \cdots \xleftarrow{d_{n-1}} P_n \xleftarrow{d_n} \cdots \tag{1}$$

which is exact in degree less than or equal to k, and each P_i is a projective Γ-module. A resolution (1) is called minimal if $d_i(P_{i+1}) \subset I(\Gamma) \cdot P_i$ for all $i \geq 0$ where $I(\Gamma) = \ker(\eta \colon \Gamma \to K)$

Proposition 0.1. *Let* $0 \leftarrow M \xleftarrow{\epsilon} P_0 \xleftarrow{d_0} P_1 \xleftarrow{d_1} P_2 \xleftarrow{d_2} \cdots \xleftarrow{d_{n-1}} P_n \xleftarrow{d_n} \cdots$ *be a minimal resolution of* M *by projective* Γ *modules. Then* $\mathrm{Ext}^s_\Gamma(M,K) \cong \mathrm{Hom}(p_s, K)$.

We study the explicit algorithm to compute such a resolution.

Definition 0.2. Let P be a graded Γ-module. $\{\mathbf{g}_1, \ldots, \mathbf{g}_N\} \subset P$ is (Γ, k)-generating set of P if inclusion

$$\langle \mathbf{g}_1, \ldots, \mathbf{g}_N \rangle \hookrightarrow P$$

induces an isomorphism of K-vector spaces in degree less than or equal to k.

Suppose that we have a part of the resolution (1)

$$P_{n-1} \xleftarrow{d_{n-1}} P_n \xleftarrow{d_n} P_{n+1}. \tag{2}$$

We also suppose that we have a Γ-basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_N\}$ (resp. $\{\mathbf{e}'_1, \ldots, \mathbf{e}'_M\}$) of P_n (resp. P_{n+1}). That is,

$$P_n \cong \bigoplus_{i=1}^N \Gamma \mathbf{e}_i \text{ and } P_{n+1} \cong \bigoplus_{i=1}^M \Gamma \mathbf{e}'_i.$$

We assume that $\{d_n(\mathbf{e}'_1), \ldots, d_n(\mathbf{e}'_M)\}$ is minimal generating set in the sense of Definition 2.17. To extend the resolution (2), we need to know an (Γ, k)-generating set $\{\mathbf{h}_1, \ldots, \mathbf{h}_L\}$ of

$$\ker \left[d_n \colon \bigoplus_{i=1}^M \Gamma \mathbf{e}'_i \to \bigoplus_{i=j}^N \Gamma \mathbf{e}_j \right].$$

Section 3 gives us an algorithm to compute it. Especially, we can choose $\{\mathbf{h}_1, \ldots, \mathbf{h}_L\}$ as a minimal generating set in the sense of Definition 2.17.

Set $P_{n+2} = \bigoplus_{i=1}^L \Gamma \mathbf{e}''_i$, $|\mathbf{e}''_i| = |\mathbf{h}_i|$ for $i = 1, \ldots, L$. We define the Γ-homomorphism

$$d_{n+1} \colon \bigoplus_{i=1}^L \Gamma \mathbf{e}''_i \to \bigoplus_{i=1}^M \Gamma \mathbf{e}'_i$$

by $d_{n+1}(\mathbf{e}''_i) = \mathbf{h}_i$. Then we have a longer resolution

$$P_{n-1} \xleftarrow{d_{n-1}} P_n \xleftarrow{d_n} P_{n+1} \xleftarrow{d_{n+1}} P_{n+2}$$

which is minimal and exact in degree less than or equal to k (see Proposition 2.19). Thus we have $\mathrm{Ext}^{n+1,t}_\Gamma(M,K) \cong \mathrm{Hom}^t_\Gamma(P_{n+1}, K)$ for $t \leq k$.

1 Noncommutative ring

The most important theory in computational algebra is Gröbner basis theory. In this paper, we are interested in noncommutative algebras. Thus we need to construct noncommutative Gröbner basis theory. It is now used in various fields. Such fields are listed in the introduction of [2]. In this section, we give the noncommutative Gröbner basis theory following the commutative theory given in [1].

1.1 Monomial order and division algorithm

Let K be a field and $R = K\langle x_1, x_2, \cdots \rangle$ be a free non commutative graded K-algebra with grading $|x_i| = \deg x_i = a_i > 0$. We call an element $X := x_{i_1} x_{i_2} \ldots x_{i_n}$ of R a *monomial* of R. Similarly, we call an element cX of R a *term* of R where $c \in K$ and X is a monomial of R.

Definition 1.1. Let $<$ be a well-ordering on the set of the monomials of R. $<$ is a *monomial ordering* of R if the following conditions are satisfied.

1. If U, V, X, Y are monomials with $X < Y$, then $UXV < UYV$.
2. For monomials X and Y, if $X = UYV$ for some monomials U, V with $U \neq 1$ or $V \neq 1$, then $Y < X$. (Hence $1 < X$ for all monomial X with $X \neq 1$.)

Remark. If R is a commutative ring $K[x_1, \ldots, x_n]$, then any ordering on the set of monomial which satisfies above two condition is a well-ordering. On the contrary, if R is a noncommutative ring, being a well-ordering does not follow from the above two condition.

Example 1.2. We define a monomial ordering on R as follows. Let $X = x_{a_1} \cdots x_{a_k}$ and $Y = x_{b_1} \cdots x_{b_l}$ be monomials of R. Then, $X \geq Y$ if $k > l$ or, $k = l$ and the *left-most* nonzero entry of $(a_1 - b_1, \ldots, a_k - b_k)$ is positive.

In this section, we fix a monomial ordering $<$ of R. For a non-zero polynomial $f \in R$, we may write f as a linear combination of monomials of R. That is,

$$f = c_1 X_1 + \cdots + c_m X_m$$

where $c_i \in K \setminus \{0\}$, X_i is a monomial satisfying $X_1 > X_2 > \cdots > X_m$. We define:

- $\mathrm{lm}(f) = X_1$, the *leading monomial* of f;
- $\mathrm{lc}(f) = a_1$, the *leading coefficient* of f;
- $\mathrm{lt}(f) = a_1 X_1$, the *leading term* of f.

We also define $\mathrm{lp}(0) = \mathrm{lc}(0) = \mathrm{lt}(0) = 0$.

DEFINITION 1.3. Let X and Y be monomials of R. X is divisible by Y if there exists monomials U, V of R such that $X = UYV$.

Let $(f_1, \dots, f_n)$ be ordered n-tuple of R. We study the *division* of $f \in R$ by $(f_1, \dots, f_n)$. First we consider the special case of the division of f by g, where $f, g \in R$.

DEFINITION 1.4. Given f, g, h in R with $g \neq 0$, we says that f *reduces to h modulo g in one step*, written

$$f \xrightarrow{g} h,$$

if $\mathrm{lm}(g)$ divides a non-zero monomial X_i that appears in f and

$$h = f - \frac{c_i X_i}{\mathrm{lt}(g)} g.$$

EXAMPLE 1.5. Set $f = x_1x_2x_3x_1 + x_1x_2, g = x_1x_2 + x_2 \in R$. Also, let the order be that defined in Example 1.2. Then

$$f \xrightarrow{g} -x_2x_3x_1 + x_1x_2 \xrightarrow{g} -x_2x_3x_1 - x_2.$$

We extend the process defined above to more general setting.

DEFINITION 1.6. Let f, h be polynomials in R and $F = \{f_\lambda\}_{\lambda \in \Lambda}$ be a family of non-zero polynomials. We say that f *reduces to h modulo F, denoted*

$$f \xrightarrow{F}_+ h,$$

if there exists a sequences of indices $\lambda_1, \lambda_2, \dots, \lambda_t \in \Lambda$ and a sequences of polynomials $h_1, \dots, h_t \in R$ such that

$$f \xrightarrow{f_{\lambda_1}} h_1 \xrightarrow{f_{\lambda_2}} h_2 \xrightarrow{f_{\lambda_3}} \cdots \xrightarrow{f_{\lambda_{t-1}}} h_{t-1} \xrightarrow{f_{\lambda_t}} h_t = h.$$

DEFINITION 1.7. A polynomial $r \in R$ is called reduced with respect to $F = \{f_\lambda\}_{\lambda \in \Lambda}$ if $r = 0$ or no monomial that appears in r is divisible by any one of the $\mathrm{lm}(f_\lambda), \lambda \in \Lambda$. If $f \xrightarrow{F}_+ r$ and r is reduced with respect to F, then we call r a remainder for f with respect to F.

PROPOSITION 1.8. *Let f be a polynomial in R and Let $F = \{f_\lambda\}_{\lambda \in \Lambda}$ be a family of non-zero polynomials in R. Then f can be written as*

$$f = \sum_{i=1}^{t} c_i p_i f_{\lambda_i} q_i + r$$

where $c_i \in K, p_i, q_i, r \in R, i = 1, \dots, t$ such that r is reduced with respect to F and

$$\mathrm{lm}(f) = \max\left\{ \max_{1 \le i \le t} \mathrm{lm}(p_i f_{\lambda_i} q_i), \mathrm{lm}(r) \right\}.$$

Unfortunately, this decomposition depends on the choice of the order of $F = \{f_\lambda\}_{\lambda\in\Lambda}$, and $f \in \langle f_\lambda | \lambda \in \Lambda\rangle$ does not imply $f \xrightarrow{F}_+ 0$. Here $\langle f_\lambda | \lambda \in \Lambda\rangle$ denotes the two-side ideal generated by $F = \{f_\lambda\}_{\lambda\in\Lambda}$. We can overcome this difficulty of remainders by choosing a Gröbner basis defined as:

Definition 1.9. A family of non-zero polynomials $G = \{g_\lambda\}_{\lambda\in\Lambda}$ contained in a two-side ideal I of R, is a called *Gröbner basis* for I if for all $f \in I \setminus \{0\}$, there exists $\lambda \in \Lambda$ satisfying that $\mathrm{lp}(g_\lambda)$ divides $\mathrm{lp}(f)$.

Remark. Since R is not Noetherian ring, Gröbner basis is not necessarily a finite set.

Theorem 1.10. *Let I be a non-zero two-side ideal of R. The following statements are equivalent for a set of non-zero polynomials $G = \{g_\lambda\}_{\lambda\in\Lambda} \subset I$.*

1. *G is a Gröbner basis for I.*
2. *$f \in I$ if and only if $f \xrightarrow{G}_+ 0$.*
3. *$f \in I$ if and only if $f = \sum_{i=1}^{t} u_i g_{\lambda_i} v_i$ with $\mathrm{lp}(f) = \max_{1\le i\le t}(\mathrm{lp}(u_i)\mathrm{lp}(g_{\lambda_i})\mathrm{lp}(v_i))$ where $u_i, v_i \in R$.*
4. *A basis of the space R/I consists of the coset of all the monomials X in R which is reduced with respect to G.*

Proof. ($4 \Rightarrow 2$) Set $f \in R$. By Proposition 1.8, there exists a reduced polynomial $r \in R$ such that $f \xrightarrow{G}_+ r$. Then r is a linear combination of reduced monomials with respect to R. Since f and r represent the same element in R/I, f is zero in R/I if and only if $r = 0$ in R.

For the remaining part of the proof, see [1, Theorem 1.6.2 and Proposition 2.1.6]. □

Let $G = \{g_\lambda\}_{\lambda\in\Lambda}$ be a Gröbner basis. For any $f \in R$, let r be a reduced polynomial in R such that $f \xrightarrow{G}_+ r$. Theorem 1.10 implies that r is unique. We call r the normal form of f with respect to G, denoted $N_G(f)$.

1.2 S-polynomials

The key to compute a Gröbner basis is the S-polynomial. In the contrast to the commutative case, the S-polynomial of noncommutative polynomials f and g in R is not unique.

Definition 1.11. Let f, g be polynomials in R. Set $\mathrm{lm}(f) = x_{i_1} \dots x_{i_n}$ and $\mathrm{lm}(g) = x_{j_1} \dots x_{j_m}$. We define the coefficient set of the S-polynomial of f and g, denoted $C(f,g)$ by

$$\begin{aligned} C(f,g) &= \left\{ (x_{a_1} \dots x_{a_\alpha}, 1, x_{c_1} \dots x_{c_\gamma}) \in R^3 \;\middle|\; \begin{array}{c} (a_1, \dots, a_\alpha) = (j_1, \dots, j_\alpha), \\ (i_1, \dots, i_{m-\alpha}) = (j_{\alpha+1}, \dots, j_m) \\ (i_{m-\alpha+1}, \dots, i_n) = (c_1, \dots, c_\gamma) \end{array} \right\} \\ &\cup \left\{ (1, x_{b_1} \dots x_{b_\beta}, x_{c_1} \dots x_{c_\gamma}) \in R^3 \;\middle|\; \begin{array}{c} (i_1, \dots, i_\beta) = (b_1, \dots, b_\beta), \\ (i_{\beta+1}, \dots, i_{\beta+m}) = (j_1, \dots, j_m) \\ (i_{\beta+m+1}, \dots, i_n) = (c_1, \dots, c_\gamma) \end{array} \right\}. \end{aligned}$$

Let f, g be polynomials and $(z, p, q) \in C(f, g)$. We define the *S-polynomial* of f and g associated with (z, p, q), denoted $S(f, g; z, p, q)$, by

$$S(f, g; z, p, q) = zf - pgq.$$

Theorem 1.12 (Buchberger's theorem for noncommutative algebra). *Let $G = \{g_\lambda\}_{\lambda \in \Lambda}$ be a family of non-zero polynomials in R. Then G is a Gröbner basis for the ideal $I = \langle g_\lambda | \lambda \in \Lambda \rangle$ if and only if for all $\lambda, \gamma \in \Lambda$, and for all $(z, p, q) \in C(g_\lambda, g_\gamma)$,*

$$S(g_\lambda, g_\gamma; z, p, q) \xrightarrow{G}_+ 0.$$

In [2], there are no explicit description of the proof of Buchberger's theorem for noncommutative algebra. We give the proof according to the proof for commutative case by [1]. Before we can prove this result, we need one preliminary lemma.

Lemma 1.13. *Let $f_1, \dots, f_s \in R$ be polynomials such that $\mathrm{lp}(f_i) = X \neq 0$ for all $i = 1, \dots, s$. Let $f = \sum_{i=1}^s c_i f_i$ with $c_i \in K$, $i = 1, \dots, s$. If $\mathrm{lp}(f) < X$, then f is a linear combination with coefficients in K, of $S(f_i, f_j; 1, 1, 1)$, $1 \leq i, j \leq s$.*

Proof. See the proof of [1, Lemma 1.7.5]. □

Proof of Theorem 1.12. If $G = \{g_\lambda\}_{\lambda \in \Lambda}$ is a Gröbner basis of $I = \langle g_\lambda | \lambda \in \Lambda \rangle$, then $S(g_\lambda, g_\gamma; z, p, q) \xrightarrow{G}_+ 0$ by Theorem 1.10, since $S(g_\lambda, g_\gamma; z, p, q) \in I$.

Conversely, let us assume that $S(g_\lambda, g_\gamma; z, p, q) \xrightarrow{G}_+ 0$ for all $\lambda \neq \gamma \in \Lambda, (z, p, q) \in C(g_\lambda, g_\gamma)$. We will use Theorem 1.10, 3 to show that G is a Gröbner basis for I. Set $f \in I$. Then f can be written in many ways as linear combination of the g_λ's. We choose to write $f = \sum_{i=1}^t u_i g_{\lambda_i} v_i$, $u_i, v_i \in R$, with

$$X = \max_{1 \leq i \leq t} (\mathrm{lp}(u_i) \mathrm{lp}(g_{\lambda_i}) \mathrm{lp}(v_i))$$

least. If $X = \mathrm{lp}(f)$, we are done. Otherwise, $\mathrm{lp}(f) < X$. We will find the representation of f with a smaller X. Let $S = \{i | \mathrm{lp}(u_i) \mathrm{lp}(g_{\lambda_i}) \mathrm{lp}(v_i) = X\}$. For $i \in S$, write $u_i = c_i X_i +$

lower terms and $v_i = Y_i +$ lower terms. Set $g = \sum_{i \in S} c_i X_i g_i Y_i$. Then, $\mathrm{lp}(X_i g_{\lambda_i} Y_i) = X$, for all $i \in S$, but $\mathrm{lp}(g) < X$. By lemma 1.13, there exists $d_{i,j} \in K$ such that

$$g = \sum_{i,j \in S, i \neq j} d_{i,j} S(X_i g_{\lambda_i} Y_i, X_j g_{\lambda_j} Y_j; 1, 1, 1).$$

Now, by the definition of S, for $i, j \in S$ we have

$$\begin{aligned} X &= X_i g_{\lambda_i} Y_i \\ &= X_j g_{\lambda_j} Y_j \\ &= \mathrm{lcm}(X_i g_{\lambda_i} Y_i, X_j g_{\lambda_j} Y_j), \end{aligned}$$

so it follows that,

$$\begin{aligned} S(X_i g_{\lambda_i} Y_i, X_j g_{\lambda_j} Y_j; 1, 1, 1) &= X_i g_{\lambda_i} Y_i - X_j g_{\lambda_j} Y_j \\ &= U_{ij} S(g_{\lambda_i}, g_{\lambda_j}; z, p, q) V_{ij} \end{aligned}$$

for some monomials U_{ij}, V_{ij} in R and $(z, p, q) \in C(g_{\lambda_i}, g_{\lambda_j})$. By the hypothesis, $S(g_{\lambda_i}, g_{\lambda_j}; z, p, q) \xrightarrow{G}_+ 0$, thus $S(X_i g_{\lambda_i} Y_i, X_j g_{\lambda_j} Y_j; 1, 1, 1) \xrightarrow{G}_+ 0$. This gives a presentation

$$S(X_i g_{\lambda_i} Y_i, X_j g_{\lambda_j} Y_j; X) = \sum_{\nu=1}^{s} u_{ij\nu} g_{\lambda_n u} v_{ij\nu},$$

such that, by Proposition 1.8,

$$\begin{aligned} \max_{1 \leq \nu \leq s} (\mathrm{lp}(u_{ij\nu}) \mathrm{lp}(g_{\lambda_n u}) \mathrm{lp}(v_{ij\nu})) &= \mathrm{lp}(S(X_i g_{\lambda_i} Y_i, X_j g_{\lambda_j} Y_j; 1, 1, 1)) \\ &< \max(\mathrm{lp}(X_i g_{\lambda_i} Y_i), \mathrm{lp}(X_j g_{\lambda_j} Y_j))) = X. \end{aligned}$$

Substituting these expressions into g above, and g into f, we get a desired contradiction.

□

2 Modules over a noncommutative ring

2.1 Gröbner basis for modules

Let K and R be as above. Let $\mathbf{e}_1, \ldots, \mathbf{e}_m$ be standard basis of R^m,

$$\mathbf{e}_1 = (1, 0, \ldots, 0), \mathbf{e}_2 = (0, 1, \ldots, 0), \ldots, \mathbf{e}_m = (0, 0, \ldots, 0, 1).$$

Then, by a *monomial* in R^m we mean a vector of the type $X\mathbf{e}_i$ $(1 \leq i \leq m)$, where X is a monomial in R.

Example 2.1. $(0, x_1x_3x_1, 0), (0, 0, x_2)$ are monomials in R^3 but $(x_1, x_2, 0)$ is not.

Similarly, by a *term*, we mean a vector of the type $c\mathbf{X}$, where $c \in K \setminus \{0\}$ and $\mathbf{X}$ is a monomial.

Example 2.2. $(0, 5x_1x_1x_3, 0, 0)$ is a term of R^4 but not a monomial.

If $\mathbf{X} = cX\mathbf{e}_i$ and $\mathbf{Y} = dY\mathbf{e}_j$ are terms of R^m, we say that $\mathbf{X}$ divides $\mathbf{Y}$ provided $i = j$ and there is a monomial Z in R such that $Y = ZX$. We write

$$\frac{\mathbf{Y}}{\mathbf{X}} = \frac{dY}{cX} = \frac{d}{c}Z.$$

Example 2.3. $(0, x_1x_3, 0)$ divides $(0, x_1x_1x_3, 0)$ but does not divide $(0, x_3, 0)$ or $(x_2x_1x_3, 0, 0)$, so we have

$$\frac{(0, x_1x_1x_3, 0)}{(0, x_1x_3, 0)} = \frac{x_1x_1x_3}{x_1x_3} = x_1.$$

If there exists a monomial $Z \in R$ such that $\mathbf{X} = Z\mathbf{Y}$ or $\mathbf{Y} = Z\mathbf{X}$, then we define the least common multiple of $\mathbf{X}$ and $\mathbf{Y}$, denoted $\operatorname{lcm}(\mathbf{X}, \mathbf{Y})$, by

$$\operatorname{lcm}(\mathbf{X}, \mathbf{Y}) = \begin{cases} Z\mathbf{Y} & \text{if } \mathbf{X} = Z\mathbf{Y} \\ Z\mathbf{X} & \text{if } \mathbf{Y} = Z\mathbf{X}. \end{cases}$$

Otherwise we define $\operatorname{lcm}(\mathbf{X}, \mathbf{Y}) = 0$.

Definition 2.4. By a term order on the monomials of R^m, we mean a well-ordering $<$ on these monomials satisfying the following conditions:

1. If $\mathbf{X} < \mathbf{Y}$ then $Z\mathbf{X} < Z\mathbf{Y}$ for all monomials $\mathbf{X}, \mathbf{Y}$ and every monomial Z in R.

2. $\mathbf{X} < Z\mathbf{X}$, for every monomial $\mathbf{X}$ in R^m and monomial $Z \neq 1$ in R.

We define an order on R^m using an order of R.

Definition 2.5 (POT (position over term)). For monomials $\mathbf{X} = X\mathbf{e}_i, \mathbf{Y} = Y\mathbf{e}_j \in R^m$, where X, Y are monomials in R, we say that

$$\mathbf{X} < \mathbf{Y} \text{ if and only if } \begin{cases} i > j \\ \text{or} \\ i = j \text{ and } X < Y. \end{cases}$$

We now adopt some notation. We first fix a term order $<$ on the monomials of R^m. Then for all $\mathbf{f} \in R^m$, with $\mathbf{f} \neq 0$, we may write

$$\mathbf{f} = a_1\mathbf{X}_1 + a_2\mathbf{X}_2 + \cdots + a_i\mathbf{X}_i + \cdots + a_r\mathbf{X}_r,$$

where, for $1 \leq i \leq r$, $a_i \in K \setminus \{0\}$ and $\mathbf{X}_i$ is a monomial in R^m satisfying $\mathbf{X}_1 > \mathbf{X}_2 > \cdots > \mathbf{X}_r$. We define

- $\mathrm{lm}(\mathbf{f}) = \mathbf{X}_1$, the leading monomial of $\mathbf{f}$.

- $\mathrm{lc}(\mathbf{f}) = a_1$, the leading coefficient of $\mathbf{f}$.

- $\mathrm{lt}(\mathbf{f}) = a_1\mathbf{X}_1$, the leading term of $\mathbf{f}$.

We define $\mathrm{lm}(\mathbf{0}) = \mathrm{lt}(\mathbf{0}) = \mathbf{0}$ and $\mathrm{lc}(\mathbf{0}) = 0$.

Remark. lm, lc and lt are multiplicative in the following sense: $\mathrm{lm}(f\mathbf{g}) = \mathrm{lp}(f)\mathrm{lm}(\mathbf{g})$, $\mathrm{lc}(f\mathbf{g}) = \mathrm{lc}(f)\mathrm{lc}(\mathbf{g})$ and $\mathrm{lt}(fg) = \mathrm{lt}(f)\mathrm{lt}(\mathbf{g})$, for all $f \in R$ and $\mathbf{g} \in R^m$.

Similar to the reduction of polynomials, we introduce the reduction of vectors.

Definition 2.6. Given vectors $\mathbf{f}, \mathbf{g}, \mathbf{h}$ in R^m with $\mathbf{g} \neq 0$, we says that $\mathbf{f}$ *reduces to* $\mathbf{h}$ *modulo* $\mathbf{g}$ *in one step*, written

$$\mathbf{f} \xrightarrow{\mathbf{g}} \mathbf{h},$$

if $\mathrm{lt}(\mathbf{g})$ divides a non-zero term $\mathbf{X}_i$ that appears in $\mathbf{f}$ and

$$\mathbf{h} = \mathbf{f} - \frac{\mathbf{X}_i}{\mathrm{lt}(\mathbf{g})}\mathbf{g}.$$

Example 2.7. Set $\mathbf{f} = (x_1x_2x_3x_1 + x_1x_2, x_1, 0), \mathbf{g} = (x_1x_2 + x_2, 0, x_3) \in R^3$. Also, let the order be POT. Then,

$$\mathbf{f} \xrightarrow{\mathbf{g}} (-x_2x_3x_1 + x_1x_2, x_1, -x_3x_3x_1) \xrightarrow{\mathbf{g}} (x_2x_3x_1 + x_2, x_1, x_3x_3x_1 + x_3).$$

Let $\Omega = \{\omega_\lambda\}_{\lambda\in\Lambda}$ be a subset of R and $\langle\Omega\rangle$ denote the two-side ideal of R generated by Ω. We suppose that Ω is a Gröbner basis. For a positive integer k, set $\Omega(k) = \Omega \cup \{g \in R||g| > k\}$. Then $\Omega(k)$ is also a Gröbner basis. We define a map $N_{\Omega,k} \colon \bigoplus_{i=1}^m R\mathbf{e}_i \to \bigoplus_{i=1}^m R\mathbf{e}_i$ by

$$N_{\Omega,k}(f_1, \ldots, f_s) = (N_{\Omega(k-|\mathbf{e}_1|)}(f_1), \ldots, N_{\Omega(k-|\mathbf{e}_m|)}(f_m)).$$

Definition 2.8. Let $\mathbf{f}, \mathbf{h}$ and $\mathbf{f}_1, \ldots, \mathbf{f}_s$ be vectors in R^m with $\mathbf{f}_i \neq 0$, and set $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$. We say that $\mathbf{f}$ (Ω, k)-*reduces to* $\mathbf{h}$ modulo F, denoted

$$\mathbf{f} \xrightarrow{F}_{\Omega,k} \mathbf{h},$$

if there exists a sequences of indices $i_1, i_2, \ldots, i_t \in \{1, \ldots, s\}$ and a sequences of vectors $\mathbf{h}_1, \ldots, \mathbf{h}_t \in R$ such that

$$\mathbf{f} \xrightarrow{\mathbf{f}_{i_1}} \mathbf{h}_1 \xrightarrow{\mathbf{f}_{i_2}} \mathbf{h}_2 \xrightarrow{\mathbf{f}_{i_3}} \cdots \xrightarrow{\mathbf{f}_{i_{t-1}}} \mathbf{h}_{t-1} \xrightarrow{\mathbf{f}_{i_t}} \mathbf{h}_t.$$

and $N_{\Omega,k}(\mathbf{h}_t) = \mathbf{h}$.

A vector $\mathbf{r} \in R$ is called (Ω, k)-*reduced with respect to* $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_t\}$ if $\mathbf{r} = 0$ or no monomial that appears in $\mathbf{r}$ is divisible by any one of the $\mathrm{lm}(\mathbf{f}_i), i \in \{1, \ldots, t\}$ and $N_{\Omega,k}(\mathbf{r}) = \mathbf{r}$.

2.2 (Ω, k)-Gröbner basis

Definition 2.9. Let $\mathbf{f}_1, \ldots, \mathbf{f}_s$ be vectors in $\bigoplus_{i=1}^m R\mathbf{e}_i$. A submodule M of $\bigoplus_{i=1}^m R\mathbf{e}_i$ is (Ω, k)-generated by $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$, denoted $M = \langle F \rangle_{\Omega,k} = \langle \mathbf{f}_1, \ldots, \mathbf{f}_s \rangle_{\Omega,k}$, if

$$M = \left\{ \sum_{i=1}^{t} p_i \mathbf{f}_i + \sum_{i=1}^{m} q_i \mathbf{e}_i \,\middle|\, p_i \in R, q_i \in \langle \Omega(k - |\mathbf{e}_i|) \rangle \right\}.$$

Definition 2.10. A set of non-zero vectors $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\} \subset \bigoplus_{i=1}^m R\mathbf{e}_i$, is a called (Ω, k)-*Gröbner basis* for $M = \langle \mathbf{g}_1, \ldots, \mathbf{g}_t \rangle_{\Omega,k}$ if for all $\mathbf{f} \in M$ such that $\mathbf{f} \neq 0$, one of the following two conditions is satisfied.

1. There exists $i \in \{1, \ldots, t\}$ satisfying that $\mathrm{lm}(\mathbf{g}_i)$ divides $\mathrm{lm}(\mathbf{f})$.
2. There exists $j \in \{1, \ldots, m\}$ and $q \in \langle (\Omega(k - |\mathbf{e}_j|)) \rangle$ such that $\mathrm{lm}(q\mathbf{e}_j)$ divides $\mathrm{lm}(\mathbf{f})$.

Here $\langle \mathrm{Lt}(\Omega(k - |\mathbf{e}_i|)) \rangle$ denotes the two side ideal generated by $\{\mathrm{lm}(g)\mathbf{e}_i | g \in \Omega(k - |\mathbf{e}_i|)\}$.

Proposition 2.11. *Let* $\mathbf{f}$ *be a vector in* $\bigoplus_{i=1}^m R\mathbf{e}_i$ *and Let* $G = \{\mathbf{g}_1 \ldots, \mathbf{g}_t\} \subset \bigoplus_{i=1}^m R\mathbf{e}_i$ *be a* (Ω, k)*-Gröbner basis. Then there exists a unique* $\mathbf{r} \in \bigoplus_{i=1}^m R\mathbf{e}_i$ *such that* $\mathbf{r}$ *is* (Ω, k)*-reduced with respect to* G *and*

$$f = \sum_{i=1}^{t} p_i \mathbf{f}_i + \sum_{i=1}^{m} q_i \mathbf{e}_i + r$$

where $p_i \in R, i = 1, \ldots, t$ *and* $q_i \in \langle \Omega(k - |\mathbf{e}_i|) \rangle, i = 1, \ldots, m$ *with*

$$\mathrm{lm}(\mathbf{f}) = \max \left\{ \max_{1 \le i \le t} \mathrm{lm}(p_i \mathbf{f}_i),\ \max_{1 \le i \le m} \mathrm{lm}(q_i \mathbf{e}_i),\ \mathrm{lm}(r) \right\}.$$

The proof is straightforward. See [1, Theorem 1.5.9. and Theorem 1.6.7.]. Let $\mathbf{f}$ and $\mathbf{g}$ be vectors in R^m. The S-vector of $\mathbf{f}$ and $\mathbf{g}$, denoted $S(\mathbf{f}, \mathbf{g})$, is

$$S(\mathbf{f}, \mathbf{g}) := \frac{\mathrm{lcm}(\mathrm{lt}(\mathbf{f}), \mathrm{lt}(\mathbf{g}))}{\mathrm{lt}(\mathbf{f})} \mathbf{f} - \frac{\mathrm{lcm}(\mathrm{lt}(\mathbf{f}), \mathrm{lt}(\mathbf{g}))}{\mathrm{lt}(\mathbf{g})} \mathbf{g}.$$

Definition 2.12. Let $\mathbf{f} \in M$ be a vector and $g \in R$ be polynomial. Set $\mathrm{lm}(\mathbf{f}) = x_{i_1} x_{i_2} \ldots x_{i_k} \mathbf{e}_{i_\mathbf{f}}$ and $\mathrm{lp}(g) = x_{j_1} x_{j_2} \ldots x_{j_h}$. We define the coefficient set of S-vectors of $\mathbf{f}$ with g, denoted $C(\mathbf{f}; g)$ as

$$\begin{aligned} & \{(1, x_{i_1} \ldots x_{i_\delta}, x_{i_{\delta+k+1}} \ldots x_{i_k}) \in R^3 | (i_{\delta+1}, \ldots, i_{\delta+k}) = (j_1, \ldots, j_k)\} \\ \cup \quad & \{(x_{j_1} \ldots x_{j_\delta}, 1, x_{i_{h-\delta+1}} \ldots x_{i_k}) \in R^3 | (i_1, \ldots, i_{h-\delta}) = (j_{\delta+1}, \ldots, j_h)\}. \end{aligned}$$

The S-vector of $\mathbf{g}_i$ and $\omega \in \Omega$, with regard to $(z, p, q) \in C(\mathbf{g}_i; \omega)$ is, given by

$$S(\mathbf{g}_i, \omega; z, p, q) = z\mathbf{g}_i - p\omega q \mathbf{e}_{\mu_i}$$

where μ_i represents a position of the non-zero coordinate of $\mathbf{g}_i$.

Theorem 2.13. *Let $G = \{\mathbf{g}_1 \ldots, \mathbf{g}_t\}$ be a set of non-zero vectors in $\bigoplus_{i=1}^m R\mathbf{e}_i$. Then G is a (Ω, k)-Gröbner basis for the submodule $M = \langle \mathbf{g}_1 \ldots, \mathbf{g}_t \rangle_{\Omega,k}$ if and only if for all $i, j \in \{1, \ldots, t\}$*

$$S(\mathbf{g}_i, \mathbf{g}_j) \xrightarrow{G}_{\Omega,k} \mathbf{0},$$

and for all $i \in \{1, \ldots, t\}, \omega \in \Omega$ and $(z, p, q) \in C(\mathbf{g}_i, \omega)$,

$$S(\mathbf{g}_i; z, p, q) \xrightarrow{G}_{\Omega,k} \mathbf{0}.$$

The proof is basically the same as the one for Theorem 1.12.

Let $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_r\}$ be a (Ω, k)-Gröbner basis. For any $\mathbf{f} \in \bigoplus_{i=1}^m R\mathbf{e}_i$, let $\mathbf{r}$ be a (Ω, k)-reduced vector with respect to G such that $\mathbf{f} \xrightarrow{G}_{+} \mathbf{r}$. Proposition 2.11 implies that $\mathbf{r}$ is unique. We call $\mathbf{r}$ the (Ω, k)-normal form of $\mathbf{f}$ with respect to G, denoted $N_{G,\Omega,k}(\mathbf{f})$.

2.3 Projective resolution

The proof of Proposition 2.14 and Theorem 2.15 in this section is based on the arguments in [1, Section 3.4.]. Let M be a graded projective R-module generated by $\mathbf{e}_1, \ldots, \mathbf{e}_s$. That is,

$$M = \bigoplus_{i=1}^{m} R\mathbf{e}_i.$$

Let $\rho_{\Omega,k}$ be a natural projection

$$\rho_{\Omega,k} \colon \bigoplus_{i=1}^{m} R\mathbf{e}_i \to \bigoplus_{i=1}^{m} R/\langle \Omega(k - |\mathbf{e}_i|) \rangle \mathbf{e}_i$$

Let $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ be a subset of M. We define the graded R-module N as

$$N = \bigoplus_{i=1}^{s} R\mathbf{e}'_j.$$

with grading $|\mathbf{e}'_j| = |\mathbf{f}_j|$. We also define the degree preserving R-homomorphism $\varphi \colon N \to M$ by $\varphi_F(\mathbf{e}'_j) = \mathbf{f}_j$. We call the kernel of composite $\rho_{\Omega,k} \circ \varphi_F$ the (Ω, k)-syzygy of F, denoted $\mathrm{Syz}_{\Omega,k}(F)$. That is,

$$\mathrm{Syz}_{\Omega,k}(F) = \ker \rho_{\Omega,k} \circ \varphi_F = \varphi_F^{-1} \left(\bigoplus_{i=1}^{m} \Omega(k - |\mathbf{e}_i|)\mathbf{e}_i \right).$$

In this section, we study an algorithm to find a (Ω, k)-generating set of the submodule $\mathrm{Syz}_{\Omega,k}(F)$ of N for a given finite subset F of M. The next proposition shows how to compute these generating set in a special case.

Proposition 2.14. *Set* $\mathrm{Lt}(\Omega) := \{\mathrm{lm}(\omega) | \omega \in \Omega\}$. *Let* $\mathbf{X}_1, \dots, \mathbf{X}_s \in R^m$ *be monomials of* M. *Set* $\mathbf{X}_{i,j} = \mathrm{lcm}(\mathbf{X}_i, \mathbf{X}_j)$. *Then* $\mathrm{Syz}_{\mathrm{Lt}(\Omega),k}(\mathbf{X}_1, \dots, \mathbf{X}_s)$ *is* $\mathrm{Lt}(\omega)$, k*-generated by,*

$$\begin{array}{rcl} LM(\mathbf{X}_1, \dots, \mathbf{X}_s) & := & \left\{ \dfrac{\mathbf{X}_{i,j}}{\mathbf{X}_i}\mathbf{e}'_i - \dfrac{\mathbf{X}_{i,j}}{c_j\mathbf{X}_j}\mathbf{e}'_j \,\middle|\, i, j \in \{1, \dots, s\} \right\} \\ & \cup & \left\{ z\mathbf{e}'_i \,\middle|\, \begin{array}{c} i \in \{1, \dots, s\}, z \in R, {}^\exists\lambda \in \Lambda, {}^\exists p, q \in R \\ s.t.\ |\omega_\lambda| \leq k, (z, p, q) \in C(\mathbf{X}_i; \omega_\lambda) \text{ for some } z \in R. \end{array} \right\}. \end{array}$$

Proof. It is easy to see that $LM(\mathbf{X}_1, \dots, \mathbf{X}_s) \subset \mathrm{Syz}_{\mathrm{Lt}(\Omega),k}(\mathbf{X}_1, \dots, \mathbf{X}_s)$.

To prove the converse, let $(h_1, \dots, h_s) \in \mathrm{Syz}_{\mathrm{Lt}(\Omega),k}(\mathbf{X}_1, \dots, \mathbf{X}_s)$. That is,

$$h_1\mathbf{X}_1 + \cdots + h_s\mathbf{X}_x = \sum_i p_i\mathbf{e}_i \tag{3}$$

for some $p_i \in \langle \mathrm{Lt}(\Omega(k - |\mathbf{e}_i|))\rangle$ Let $\mathbf{X}$ be any monomial in $\bigoplus_{i=1}^m R\mathbf{e}_i$. Then the coefficient of $\mathbf{X}$ in $h_1\mathbf{X}_1 + \cdots + h_s\mathbf{X}_x - \sum_i p_i\mathbf{e}_i$ must be zero. Thus it is enough to consider the case for which $h_i = c_iX'_i$ with $X'_i\mathbf{X}_i = \mathbf{X}$. Let $c_{i_1}, \dots, c_{i_t}$, with $i_1 < i_2 < \cdots < i_t$ be the non-zero c_j's. Therefore, we have:

$$\begin{array}{rcl} (h_1, \dots, h_s) & = & (c_1X'_1, \dots, c_sX'_s) = c_{i_1}X'_{i_1}\mathbf{e}'_{i_1} + \cdots + c_{i_t}X'_{i_t}\mathbf{e}'_{i_t} \\ & = & c_{i_1}\dfrac{\mathbf{X}}{\mathbf{X}_{i_1}}\mathbf{e}'_{i_1} + \cdots + c_{i_t}\dfrac{\mathbf{X}}{\mathbf{X}_{i_t}}\mathbf{e}'_{i_t} \\ & = & c_{i_1}\dfrac{\mathbf{X}}{\mathbf{X}_{i_1i_2}}(\dfrac{\mathbf{X}_{i_1i_2}}{\mathbf{X}_{i_1}}\mathbf{e}'_{i_1} - \dfrac{\mathbf{X}_{i_1i_2}}{\mathbf{X}_{i_2}}\mathbf{e}'_{i_2}) \\ & & +(c_{i_1} + c_{i_2})\dfrac{\mathbf{X}}{\mathbf{X}_{i_2i_3}}(\dfrac{\mathbf{X}_{i_2i_3}}{\mathbf{X}_{i_2}}\mathbf{e}'_{i_2} - \dfrac{\mathbf{X}_{i_2i_3}}{\mathbf{X}_{i_3}}\mathbf{e}'_{i_3}) + \dots \\ & & +(c_{i_1} + \cdots + c_{i_{t-1}})\dfrac{\mathbf{X}}{\mathbf{X}_{i_{t-1}i_t}}(\dfrac{\mathbf{X}_{i_{t-1}i_t}}{\mathbf{X}_{i_{t-1}}}\mathbf{e}'_{i_{i-1}} - \dfrac{\mathbf{X}_{i_{t-1}i_t}}{\mathbf{X}_{i_t}}\mathbf{e}'_{i_t}) \\ & & (c_{i_1} + \cdots + c_{i_t})\dfrac{\mathbf{X}}{\mathbf{X}_{i_t}}\mathbf{e}'_{i_t}, \end{array}$$

If $h_1\mathbf{X}_1 + \cdots + h_s\mathbf{X}_x = 0$, then we have $c_{i_1} + \cdots + c_{i_t}$ and it follows that $(h_1, \dots, h_s) \in \langle LM(\mathbf{X}_1, \dots, \mathbf{X}_s)\rangle$. If not, there exists $i \in \{0, \dots m\}$ and $\omega \in \Omega(k - |\mathbf{e}'_i|)$ such that $\mathbf{X} = X'_{i_t}\mathbf{X}_{i_t} = p\mathrm{lm}(\omega)q\mathbf{e}_i$ where p and q are monomials in R. If $C(\mathbf{X}_{i_t}, \omega)$ is not empty, then there exists $(z, p', q) \in C(\mathbf{X}_{i_t}, \omega)$ such that $z\mathbf{X}_{i_t} = p'\mathrm{lm}(\omega)q\mathbf{e}_i$. This implies that

$$\frac{\mathbf{X}}{\mathbf{X}_{i_t}}\mathbf{e}_{i_t} = X'_{i_t}\mathbf{e}'_{i_t} = z'z\mathbf{e}'_{i_t}$$

for some monomial z' in R. If $C(\mathbf{X}_{i_t}, \omega)$ is empty, then there exists a monomial q' in R such that $X'_{i_t} = p\omega q'$. This implies that

$$\frac{\mathbf{X}}{\mathbf{X}_{i_t}}\mathbf{e}_{i_t} = X'_{i_t}\mathbf{e}'_{i_t} = p\omega q'\mathbf{e}'_{i_t} \in \bigoplus_{i=1}^s \mathrm{Lt}(\Omega(k - |\mathbf{e}'_i|))\mathbf{e}'_i.$$

Thus we have desired conclusion. □

Let $\{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ be a (Ω, k)-Gröbner basis, where we assume that the $\mathbf{g}_i$'s are monic. For $i \in \{1, \ldots, t\}$, we let $\mathrm{lm}(\mathbf{g}_i) = \mathbf{X}_i$ and for $i \neq j \in \{1, \ldots, t\}$, we let $\mathbf{X}_{ij} = \mathrm{lcm}(\mathbf{X}_i, \mathbf{X}_j)$. Then the S-polynomial of $\mathbf{g}_i$ and $\mathbf{g}_j$ is, given by

$$S(\mathbf{g}_i, \mathbf{g}_j) = \frac{\mathbf{X}ij}{\mathbf{X}_i}\mathbf{g}_i - \frac{\mathbf{X}ij}{\mathbf{X}_j}\mathbf{g}_j.$$

We note that $\mathrm{lm}(S(\mathbf{g}_i, \mathbf{g}_j)) < \mathbf{X}_{ij}$. By Proposition 2.11, we have

$$S(\mathbf{g}_i, \mathbf{g}_j) = \sum_{\nu=1}^{t} u_{ij\nu}\mathbf{g}_\nu + \sum_{\epsilon} p_\epsilon \omega_\epsilon q_\epsilon \mathbf{e}_{i_\epsilon}$$

where $u_{ij\nu}, p_\epsilon, q_\epsilon \in R, \omega_\epsilon \in \Omega(k - |\mathbf{e}_{i_\epsilon}|)$, such that

$$\max\left\{\max_{1\leq\nu\leq t}(\mathrm{lm}(u_{ij\nu})\mathrm{lm}(\mathbf{g}_\nu)), \max_{\epsilon}(\mathrm{lm}(p_\epsilon\omega_\epsilon q_\epsilon)\mathbf{e}_{i_\epsilon})\right\} = \mathrm{lm}(S(\mathbf{g}_i, \mathbf{g}_j)).$$

We now define

$$\mathbf{s}_{ij} = \frac{\mathbf{X}ij}{\mathbf{X}_i}\mathbf{e}'_i - \frac{\mathbf{X}ij}{\mathbf{X}_j}\mathbf{e}'_j - (u_{ij1}, \ldots, u_{ijt}) \in R^t.$$

It is easy to see that $\mathbf{s}_{ij} \in \mathrm{Syz}(\mathbf{g}_1, \ldots, \mathbf{g}_t)$.

Similarly, the S-polynomial of $\mathbf{g}_i$ and $\omega_\lambda, \lambda \in \Lambda$, with regard to $(z, p, q) \in C(\mathbf{g}_i; \omega_\lambda)$ is, given by

$$S(\mathbf{g}_i, \omega_\lambda; z, p, q) = z\mathbf{g}_i - p\omega_\lambda q\mathbf{e}_{\mu_i}$$

where μ_i represents a position of the non-zero coordinate of $\mathbf{g}_i$. We note that $\mathrm{lm}(S(\mathbf{g}_i, \omega_\lambda; w)) < w$. By Proposition 2.11, we have

$$S(\mathbf{g}_i, \omega_\lambda; z, p, q) = \sum_{\nu=1}^{t} h'_{i\nu}\mathbf{g}_\nu + \sum_{\epsilon} p_\epsilon\omega_\epsilon q_\epsilon \mathbf{e}_{i_\epsilon}.$$

for some $h'_{i\nu}, p_\epsilon, q_\epsilon \in R$ and $\omega_\epsilon \in \Omega(k - |\mathbf{e}_{i_\epsilon}|)$, such that

$$\max\left\{\max_{1\leq\nu\leq t}(\mathrm{lm}(h'_{i\nu})\mathrm{lm}(\mathbf{g}_\nu)), \max_{\epsilon}(\mathrm{lm}(p_\epsilon\omega_\epsilon q_\epsilon)\mathbf{e}_{i_\epsilon})\right\} = \mathrm{lm}(S(\mathbf{g}_i, \omega_\lambda; w)).$$

We now define

$$s_i(\omega_\lambda; z, p, q) = z\mathbf{e}'_i - (h'_{i1}, \ldots, h'_{it}).$$

It is also easy to see that $s_i(\omega_\lambda; z, p, q) \in \mathrm{Syz}(\mathbf{g}_1, \ldots, \mathbf{g}_t)$.

Theorem 2.15. *$\mathrm{Syz}_{\Omega,k}(\mathbf{g}_1, \ldots, \mathbf{g}_t)$ is (Ω, k)-generated by*

$$\begin{aligned} M(\mathbf{g}_1, \ldots, \mathbf{g}_t) &:= \{\mathbf{s}_{i,j} | i, j \in \{1, \ldots, t\}\} \\ &\cup \{\mathbf{s}_i(\omega_\lambda; z, p, q) | i \in \{1, \ldots, s\}, \lambda \in \lambda, |\omega_\lambda| \leq k, (z, p, q) \in C(\mathbf{g}_i, \omega_\lambda)\}. \end{aligned}$$

Proof. Suppose to the contrary that there exists $(u_1, \dots, u_t) \in \bigoplus_{i=1}^t R\mathbf{e}'_i$ such that

$$(u_1, \dots, u_t) \in \mathrm{Syz}_{\Omega,k}(\mathbf{g}_1, \dots, \mathbf{g}_t) \setminus \langle M(\mathbf{g}_1, \dots, \mathbf{g}_t)\rangle_{\Omega,k}.$$

Then we can choose such a $(u_1, \dots, u_t)$ with $\mathbf{X} = \max_{1\le i\le t}(\mathrm{lp}(u_i)\mathrm{lm}(\mathbf{g}_i))$ least. Let S be the subset of $\{1, \dots, t\}$ such that

$$S = \{i \in \{1, \dots, t\} | \mathrm{lm}(u_i)\mathrm{lm}(\mathbf{g}_i) = \mathbf{X}\}.$$

Now for each $i \in \{1, \dots, t\}$ we define u'_i as follows:

$$u'_i = \begin{cases} u_i & \text{if } i \notin S \\ u_i - \mathrm{lt}(u_i) & \text{if } i \in S. \end{cases}$$

Also, for $i \in S$, let $\mathrm{lt}(u_i) = c_i X'_i$, where $c_i \in K$ and X'_i is a monomial in R. Since $(u_1, \dots, u_t) \in \mathrm{Syz}_{\Omega,k}(\mathbf{g}_1, \dots, \mathbf{g}_t)$, we see that

$$\sum_{i\in S} c_i X'_i \mathbf{X}_i \in \bigoplus_{i=1}^m \mathrm{Lt}(\Omega(k - |\mathbf{e}_i|))\mathbf{e}_i$$

and so

$$\sum_{i\in S} c_i X'_i \mathbf{e}_i \in \mathrm{Syz}_{\mathrm{Lt}(\Omega),k}(\mathbf{X}_i | i \in S).$$

Thus, by Proposition 2.14 we have

$$\sum_{i\in S} c_i X'_i \mathbf{e}'_i = \sum_{i<j\ i,j\in S} d_{ij}(\frac{\mathbf{X}_{ij}}{\mathbf{X}_i}\mathbf{e}_i - \frac{\mathbf{X}_{ij}}{\mathbf{X}_j}\mathbf{e}_j) + \sum_{\substack{i\in S,\omega\in\Omega \\ (z,p,q)\in C(\mathbf{g}_i,\omega)}} b_{i\lambda;z}(z\mathbf{e}'_i) + \sum_{\epsilon,i\in S} p_{\epsilon i}\mathrm{lm}(\omega_{\epsilon i})q_{\epsilon i}\mathbf{e}'_i$$

for some monomials $d_{ij}, b_{i\lambda;z}, p_{\epsilon i}, q_{\epsilon i} \in R$ and $\omega_{\epsilon i} \in \Omega$. Since each coordinate of the vector in the left-hand side of the equation above is homogeneous, and since $X'_i\mathbf{X}_i = \mathbf{X}$, we can choose d_{ij} to be a constant multiple of $\frac{\mathbf{X}}{\mathbf{X}_{ij}}$. Similarly, we can choose $b_{i\lambda;z}$ to be a constant multiple of $\frac{\mathbf{X}}{z\mathbf{X}_i}$. Set $\bar{\omega}_{\epsilon i} := \omega_{\epsilon i} - \mathrm{lm}(\omega_{\epsilon i})$. Then we have

$$\begin{aligned}
(u_1, \dots, u_t) &= \sum_{i\in S} c_i X'_i \mathbf{e}_i + (u'_1, \dots, u'_t) \\
&= \sum_{i<j\ i,j\in S} d_{ij}\left(\frac{\mathbf{X}_{ij}}{\mathbf{X}_i}\mathbf{e}_i - \frac{\mathbf{X}_{ij}}{\mathbf{X}_j}\mathbf{e}_j\right) + \sum_{\substack{i\in S,\omega\in\Omega \\ (z,p,q)\in C(\mathbf{g}_i,\omega)}} b_{i\lambda;z}(z\mathbf{e}'_i) \\
&+ \sum_{\epsilon,i\in S} p_{\epsilon i}\mathrm{lm}(\omega_{\epsilon i})q_{\epsilon i}\mathbf{e}'_i + (u'_1, \dots, u'_t) \\
&= \sum_{i<j\ i,j\in S} d_{ij}\mathbf{s}_{ij} + \sum_{\substack{i\in S,\omega\in\Omega \\ (z,p,q)\in C(\mathbf{g}_i,\omega)}} b_{i\lambda;z}\mathbf{s}_i(\omega; z, p, q) \\
&+ (u'_1, \dots, u'_t) + \sum_{i<j\ i,j\in S} d_{ij}(h_{ij1}, \dots, h_{ijt}) + \sum_{\substack{i\in S,\lambda, \\ (z,p,q)\in C(\mathbf{g}_i,\omega)}} b_{i\lambda;z}(h'_{i1}, \dots, h'_{it}) \\
&+ \sum_{\epsilon,i\in S} p_{\epsilon,i}\omega_{\epsilon i}q_{\epsilon i}\mathbf{e}'_i - \sum_{\epsilon,i\in S} p_{\epsilon i}\bar{\omega}_{\epsilon i}q_{\epsilon i}\mathbf{e}'_i.
\end{aligned}$$

We define

$$\begin{aligned}(v_1,\ldots,v_t) &:= (u'_1,\ldots,u'_t) + \sum_{i<j\ i,j\in S} d_{ij}(h_{ij1},\ldots,h_{ijt}) + \sum_{\substack{i\in S,\omega\in\Omega\\(z,p,q)\in C(\mathbf{g}_i,\omega)}} b_{i\lambda;z}(h'_{i1},\ldots,h'_{it})\\ &\quad - \sum_{\epsilon,i\in S} p_{\epsilon i}\bar{\omega}_{\epsilon i}q_{\epsilon i}\mathbf{e}'_i.\end{aligned}$$

We note that $(v_1,\ldots,v_t)\in \mathrm{Syz}_{\Omega,k}(\mathbf{g}_1,\ldots,\mathbf{g}_t)\backslash\langle M(\mathbf{g}_1,\ldots,\mathbf{g}_t)\rangle_{\Omega,k}$, since $(u_1,\ldots,u_t), \mathbf{s}_{ij}, \mathbf{s}_i(\omega;z,p,q)\in \mathrm{Syz}_{\Omega,k}(\mathbf{g}_1,\ldots,\mathbf{g}_t)$ and $(u_1,\ldots,u_t)\notin\langle M(\mathbf{g}_1,\ldots,\mathbf{g}_t)\rangle_{\Omega,k}$. We will obtain the desired contradiction by proving that $\max_{1\le\nu\le t}(\mathrm{lm}(v_\nu)\mathrm{lm}(\mathbf{g}_\nu)) < \mathbf{X}$. For each $\nu\in\{1,\ldots,t\}$ we have

$$\begin{aligned}\mathrm{lm}(v_\nu)\mathrm{lm}(\mathbf{g}_\nu) &= \mathrm{lm}\left(u'_\nu + \sum_{i<j\ i,j\in S} d_{ij}\mathrm{lm}(h_{ij\nu}) + \sum_{\substack{i\in S,\omega\in\Omega\\(z,p,q)\in C(\mathbf{g}_i,\omega)}} b_{i\lambda;z}\mathrm{lm}(h'_{i\nu}) + \sum_{\epsilon} p_{\epsilon\nu}\bar{\omega}_{\epsilon\nu}q_{\epsilon\nu}\right)\mathbf{X}_\nu\\ &\le \max\left(\mathrm{lm}(u'_\nu), \max_{i<j\ i,j\in S} d_{ij}\mathrm{lm}(h_{ij\nu}), \max_{\substack{i\in S,\omega\in\Omega\\(z,p,q)\in C(\mathbf{g}_i,\omega)}} b_{i\lambda;z}\mathrm{lm}(h'_{i\nu}), \max_{\epsilon} p_{\epsilon\nu}\bar{\omega}_{\epsilon\nu}q_{\epsilon\nu},\right)\mathbf{X}_\nu\end{aligned}$$

where we assume that $p_{\epsilon\nu}\bar{\omega}_{\epsilon\nu}q_{\epsilon\nu} = 0$ if $\nu\notin S$. However, by definition of u'_ν, we have $\mathrm{lm}(u'_\nu)\mathbf{X}_\nu < X$. Also, as mentioned above, d_{ij} is a constant multiple of $\frac{\mathbf{X}}{\mathbf{X}_{ij}}$, and hence for all $i,j\in S, i<j$, we have

$$d_{ij}\mathrm{lm}(h_{ij\nu})\mathbf{X}_\nu = \frac{\mathbf{X}}{\mathbf{X}_{ij}}\mathrm{lm}(h_{ij\nu})\mathbf{X}_\nu \le \frac{\mathbf{X}}{\mathbf{X}_{ij}}\mathrm{lm}(\mathbf{s}(\mathbf{g}_i,\mathbf{g}_j)) < \frac{\mathbf{X}}{\mathbf{X}_{ij}}\mathbf{X}_{ij} = \mathbf{X}.$$

Similarly, $b_{i\lambda;z}$ is a constant multiple of $\frac{\mathbf{X}}{z\mathbf{X}_i}$, we have

$$b_{i\lambda;z}\mathrm{lm}(h'_{i\nu})\mathbf{X}_\nu = \frac{\mathbf{X}}{z\mathbf{X}_i}\mathrm{lm}(h'_{i\nu})\mathbf{X}_\nu \le \frac{\mathbf{X}}{z\mathbf{X}_i}\mathrm{lm}(\mathbf{s}_i(\omega;z,p,q)) < \frac{\mathbf{X}}{z\mathbf{X}_i}z\mathbf{X}_i = \mathbf{X}.$$

Also, by the definition of $\bar{\omega}_{\epsilon\nu}$,

$$\mathrm{lm}(p_{\epsilon\nu}\bar{\omega}_{\epsilon\nu}q_{\epsilon\nu})\mathbf{X}_\nu < \mathrm{lm}(p_{\epsilon\nu})\mathrm{lm}(\omega_{\epsilon\nu})\mathrm{lm}(q_{\epsilon\nu})\mathbf{X}_\nu = \mathbf{X}.$$

Therefore $\mathrm{lm}(v_\nu)\mathrm{lm}(\mathbf{g}_\nu) < \mathbf{X}$ for each $\nu\in\{1,\ldots,t\}$ violating the condition that $\mathbf{X} = \max_{1\le\nu\le t}(\mathrm{lm}(u_\nu)\mathrm{lm}(\mathbf{g}_\nu))$ is least. □

Finally we study the algorithm to compute $\mathrm{Syz}_{\Omega,k}(\mathbf{f}_1,\ldots,\mathbf{f}_s)$ for $\{\mathbf{f}_1,\ldots,\mathbf{f}_s\}$ be a collection of (Ω,k)-reduced vectors in $M=\bigoplus_{i=1}^u R\mathbf{e}_i$ which may not form a Gröbner basis. First we compute an (Ω,k)-Gröbner basis $\{\mathbf{g}_1,\ldots,\mathbf{g}_t\}$. We again assume that $\mathbf{g}_1,\ldots,\mathbf{g}_t$ are monic. Let

$$F = \begin{bmatrix}\mathbf{f}_1\\ \vdots\\ \mathbf{f}_s\end{bmatrix} \text{ and } G = \begin{bmatrix}\mathbf{g}_1\\ \vdots\\ \mathbf{g}_t\end{bmatrix}$$

be non-zero matrix of row vectors in M. There exists an $s \times t$ matrix S and a $t \times s$ matrix T with entries in R such that $F = N_{\Omega,k}(SG)$ and $G = N_{\Omega,k}(TF)$. Using Theorem 2.15, we can compute a generating set $\{\mathbf{s}_1, \ldots, \mathbf{s}_r\}$ for $\mathrm{Syz}_{\Omega,k}(G)$. Therefore for each $i = 1, \ldots, r$

$$\mathbf{0} = N_{\Omega,k}(\mathbf{s}_i G) = N_{\Omega,k}(\mathbf{s}_i TF) = N_{\Omega,k}((\mathbf{s}_i T)F)$$

and hence

$$\langle \mathbf{s}_i T | i = 1, \ldots, r \rangle \subset \mathrm{Syz}_{\Omega,k}(F).$$

Moreover, if we let I_s be the $s \times s$ identity matrix, we have

$$N_{\Omega,k}((I_s - ST)F) = N_{\Omega,k}(F - STF) = N_{\Omega,k}(F - SG) = \mathbf{0}$$

and hence the rows $\mathbf{r}_1, \ldots, \mathbf{r}_s$ of $I_s - TS$ are also in $\mathrm{Syz}_{\Omega,k}(F)$.

Theorem 2.16. *With the notation above we have*

$$\mathrm{Syz}_{\Omega,k}(\mathbf{f}_1, \ldots, \mathbf{f}_s) = \langle \mathbf{s}_1 T, \ldots, \mathbf{s}_r T, \mathbf{r}_1, \ldots, \mathbf{r}_s \rangle$$

The proof is straightforward and same as that of [1, Theorem 3.4.3].

To compute Ext efficiently, we need to find a generating set of the syzygy which has a small cardinality.

Definition 2.17. Let M be a submodule of $\bigoplus_{i=1}^s R\mathbf{e}_i$. $\{\mathbf{f}_1, \ldots, \mathbf{f}_r\} \subset \bigoplus_{i=1}^s R\mathbf{e}_i$ is (Ω, k)-minimal generating set of M if $M = \langle \mathbf{f}_1, \ldots, \mathbf{f}_r \rangle_{\Omega,k}$ and

$$\mathbf{f}_j \notin \langle \mathbf{f}_1, \ldots, \mathbf{f}_{j-1}, \mathbf{f}_{j+1}, \ldots, \mathbf{f}_r \rangle_{\Omega,k}$$

for any $j = 1, \ldots, r$.

Proposition 2.18. *Let $\mathbf{h}_1, \ldots \mathbf{h}_r$ be vectors in $\bigoplus_{i=1}^s R\mathbf{e}_i$. The following algorithm produces a (Ω, k)-minimal generating set of $\langle \mathbf{h}_1, \ldots \mathbf{h}_r \rangle_{\Omega,k}$.*

Algorithm 1 title

```
for $i = 0$ to $r$ do
    $G \leftarrow$ Gröbner basis of $\mathbf{h}_1, \ldots, \mathbf{h}_{i-1}, \mathbf{h}_{i+1}, \ldots \mathbf{h}_r$
    $\mathbf{h}_i \leftarrow N_{G,\Omega,k}(\mathbf{h}_i)$
end for
Let $i_1, \ldots i_{r'}$ with $i_1 \leq \cdots \leq i_{r'}$ be non-zero $\mathbf{h}_i' s$.
return $\mathbf{h}_{i_1} \ldots \mathbf{h}_{i_{r'}}$
```

Remark. In general, the output of Algorithm 1 is not a Gröbner basis even if the input is.

Proposition 2.19. *Let $\mathbf{f}_1, \ldots, \mathbf{f}_r$ be homogeneous vectors in $\bigoplus_{i=1}^{s} R\mathbf{e}_i$. If $\{\mathbf{f}_1, \ldots, \mathbf{f}_r\}$ is (Ω, k)-minimal generating set, then*

$$\mathrm{Syz}_{\Omega,k}(\mathbf{f}_1, \ldots, \mathbf{f}_s) \subset \bigoplus_{i=1}^{r} I(R)\mathbf{e}'_i.$$

Proof. Assume that there exists $\mathbf{v} = (v_1, \ldots, v_r) \in \mathrm{Syz}_{\Omega,k}(\mathbf{f}_1, \ldots, \mathbf{f}_s)$ such that $\mathbf{v} \notin \bigoplus_{i=1}^{r} I(R)\mathbf{e}'_i$. Then we have $v_i \notin I(R)$ for some $i \in \{1, \ldots, r\}$. We can suppose that v_i is homogeneous. Thus we have $v_i \in K \setminus \{0\}$. By the assumption of $\mathbf{v}$, $\sum v_i \mathbf{f}_i \in \bigoplus_{i=1}^{s} \Omega(k - |\mathbf{e}_i|)\mathbf{e}_i$. It follows that $\mathbf{f}_j \in \langle \mathbf{f}_1, \ldots, \mathbf{f}_{i-1}, \mathbf{f}_{i+1}, \ldots, \mathbf{f}_r \rangle_{\Omega,k}$. This contradicts that $\{\mathbf{f}_1, \ldots, \mathbf{f}_r\}$ is (Ω, k)-minimal generating set. □

3 Projective resolution over the noncommutative ring

In this section, we explain an algorithm to compute a minimal projective resolution. Let K, R, Ω, k be as above and set $\Gamma := R/\langle \Omega \rangle$. Suppose that we have a degree preserving Γ homomorphism d_n:

$$d_n \colon \bigoplus_{i=1}^{t} \Gamma \mathbf{e}'_i \to \bigoplus_{i=j}^{s} \Gamma \mathbf{e}_j.$$

Set $\bar{\mathbf{f}}_i = d_n(\mathbf{e}'_i)$. We can choose $\{\mathbf{f}_1, \ldots, \mathbf{f}_t\} \subset \bigoplus_{i=1}^{s} R\mathbf{e}_i$ such that

$$\rho_{\Omega,k}(\mathbf{f}_i) = \bar{\mathbf{f}}_i \in \bigoplus_{i=1}^{s} R/\langle \Omega(k - |\mathbf{e}_i|)\mathbf{e}_i \rangle \cong_k \bigoplus_{i=1}^{s} \Gamma \mathbf{e}_i.$$

Here we also suppose that $\{\mathbf{f}_1 \ldots \mathbf{f}_M\}$ is (Ω, k)-minimal generating set. Then we have a degree-preserving R-homomorphism

$$\tilde{d}_n \colon \bigoplus_{i=1}^{t} R\mathbf{e}_i \to \bigoplus_{i=1}^{s} R\mathbf{e}'_i$$

defined by $\tilde{d}_n(\mathbf{e}'_i) = \mathbf{f}_i$. Using Theorem 2.16 and Proposition 2.18, we can compute an (Ω, k)-minimal generating set $\{\mathbf{h}_1, \ldots, \mathbf{h}_r\}$ of $\mathrm{Syz}_{\Omega,k}(\mathbf{f}_1, \ldots, \mathbf{f}_t)$. Let $\bar{\mathbf{h}}_i$ be the image of $\mathbf{h}_i$ by the projection

$$\bigoplus_{i=1}^{t} R\mathbf{e}'_i \to \bigoplus_{i=1}^{t} R/\langle \Omega(k - |\mathbf{e}'_i|)\mathbf{e}'_i \rangle \cong_k \bigoplus_{i=1}^{t} \Gamma \mathbf{e}'_i.$$

Then we have a sequence of minimal Γ-homomorphisms, which is exact in degree less than or equal to k,

$$\bigoplus_{i=1}^{r} \Gamma \mathbf{e}''_i \xrightarrow{d_{n+1}} \bigoplus_{i=1}^{t} \Gamma \mathbf{e}'_i \xrightarrow{d_n} \bigoplus_{i=1}^{s} \Gamma \mathbf{e}_i$$

where $|\mathbf{e}''_i| = |\bar{\mathbf{h}}_i|$ and $d_{n+1}(\mathbf{e}''_i) = \bar{\mathbf{h}}_i$. Moreover, it follows from Proposition 2.19 that

$$d_{n+1}\left(\bigoplus_{i=1}^{r} \Gamma \mathbf{e}''_i\right) \subset I(\Gamma)\left(\bigoplus_{i=1}^{t} \Gamma \mathbf{e}'_i\right).$$

Appendix

Steenrod algebra and Gröbner basis

For details of the Steenrod algebra, see [3, chapter 4]. Let $R = \mathbb{F}_2\langle \mathrm{Sq}^1, \mathrm{Sq}^2, \cdots \rangle$ be a free noncommutative graded algebra with grading $|\mathrm{Sq}^i| = \deg \mathrm{Sq}^i = i$.

We choose a ordering on the set of monomials of R to be that of Example 1.2. Let Ω_{Adem} be a subset of R consisted of Adem relations,

$$\omega(a,b) := \mathrm{Sq}^a\mathrm{Sq}^b - \sum_{j=0}^{[a/2]} \binom{b-1-j}{a-2j} \mathrm{Sq}^{a+b-j}\mathrm{Sq}^j$$

for $0 < a < b$. We define a monomial ordering on the set of monomials of R as follows: Let $\mathrm{Sq}^{a_1} \cdots \mathrm{Sq}^{a_k}$ and $Y = \mathrm{Sq}^{b_1} \cdots \mathrm{Sq}^{b_l}$ be monomials of R. Then, $X \geq Y$ if $k > l$ or, $k = l$ and the *right-most* nonzero entry of $(a_1 - b_1, \ldots, a_k - b_k)$ is positive. It follows that $\mathrm{lm}(\omega(a,b)) = \mathrm{Sq}^a\mathrm{Sq}^b$. The Steenrod algebra is given by a quotient:

$$\mathcal{A}_2 \cong R/\langle \Omega_{\mathrm{Adem}} \rangle$$

where $\langle \Omega_{\mathrm{Adem}} \rangle$ denotes the two-side ideal of R generated by Ω_{Adem}.

Definition 3.1. A sequence $I = (a_1, \ldots, a_n) \subset \mathbb{N}$ is called an admissible sequence if $a_1, \ldots, a_n$ satisfies $a_i \geq 2a_{i+1}$ for $i = 1, \ldots, n-1$. $\mathrm{Sq}^I = \mathrm{Sq}^{a_1} \cdots \mathrm{Sq}^{a_n}$ is called an admissible element if $(a_1, \ldots, a_n)$ is an admissible sequence.

Considering the action of the Steenrod algebra on the $\mathbb{Z}/2$-cohomology of $\mathbb{R}\mathrm{P}^\infty$, it follows that Admissible elements form a basis of $\mathbb{F}_2$-vector space $\mathcal{A}_2 = R/\langle \Omega_{\mathrm{Adem}} \rangle$ [3, Theorem 4.46]. By Theorem 1.10, we have

Proposition 3.2. Ω_{Adem} *is a Gröbner basis.*

References

[1] William W. Adams and Philippe Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994. MR MR1287608 (95g:13025)

[2] Huishi Li, *Noncommutative Gröbner bases and filtered-graded transfer*, Lecture Notes in Mathematics, vol. 1795, Springer-Verlag, Berlin, 2002. MR MR1947291 (2003i:16065)

[3] John McCleary, *A user's guide to spectral sequences*, second ed., Cambridge Studies in Advanced Mathematics, vol. 58, Cambridge University Press, Cambridge, 2001. MR MR1793722 (2002c:55027)

Department of Mathematics
Kyoto University
Kyoto 606-8502
Japan

E-mail address: tomo_xi@math.kyoto-u.ac.jp